

[The Complete] Management Solution  
For Your Network

PRODUCT MANUAL

## ManageWise® 2.6

NetWare Management Agent™ 2.6  
Installation and Configuration Guide



# Novell®

ManageWise®  
MANAGEMENT SOFTWARE

## *disclaimer*

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without any obligation to notify any person or entity of such changes.

## *trademarks*

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell, NetWare, and ManageWise are registered trademarks of Novell, Inc. in the United States and other countries.

Internet Packet Exchange, IPX, IPX/SPX, NDS, NetWare 3, NetWare 4, NetWare 5, NetWare DOS Requester, NetWare Loadable Module, NLM, Sequenced Packet Exchange, SMS, SPX, Virtual Loadable Module, and VLM are trademarks of Novell, Inc.

IBM, OS/2, PC/AT, and PS/2 are registered trademarks and PC/XT is a trademark of International Business Machines Corporation. LANSpool is a registered trademark of LAN Systems, Inc. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks and Windows 95 and Windows 98 are trademarks of Microsoft Corporation. UNIX is a registered trademark of X/Open Company, Ltd.

**Copyright © 1993–98 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.**

**Novell, Inc.  
2180 Fortune Drive  
San Jose, CA 95131  
U.S.A.**

**ManageWise® 2.6  
NetWare Management Agent™ 2.6 Installation and Configuration Guide  
August 1998**

# Contents

## 1 Overview of NetWare Management Agent 2.6

About SNMP-Based Management . . . . .	2
Gathering Local Trend Information at the Server . . . . .	2
Support for Secure SNMP Transactions . . . . .	4
About NetWare Management Agent 2.6 NLM Files. . . . .	4

## 2 Installing NetWare Management Agent 2.6

NetWare Server Hardware Requirements . . . . .	8
Versions of NetWare Supported . . . . .	8
Upgrading NetWare Management Agent . . . . .	9
Installing the NetWare Management Agent 2.6 Software. . . . .	9
Installing NetWare Management Agent on Multiple Servers . . . . .	10
Installing NetWare Management Agent on SFT III Servers . . . . .	11
Updating IO Engine System and Startup Files . . . . .	11
Example of NMAX.NCF file . . . . .	11
Restarting the SFT III Servers. . . . .	12
Installing NetWare Management Agent 2.6 from Windows . . . . .	12
Loading and Unloading NetWare Management Agent 2.6 . . . . .	15
After Installation . . . . .	15
Location of the Agent Files . . . . .	16
NTREND Data Files. . . . .	16

## 3 Setting Up Secure SNMP Transactions

Using SNMP Over a NetWare Core Protocol Connection . . . . .	20
Setting Security for SNMP Management . . . . .	21
Allowing Access to a ManageWise Console and a Third-Party Management Console . . . . .	22
Configuring Security Options on a NetWare Server. . . . .	23
Configuring Community Name Options Using SNMP LOAD Commands. . . . .	24
Configuring Community Name Options Using INETCFG . . . . .	25
Setting Up the ManageWise Console for Secure SNMP Transactions . . . . .	28

## 4 Configuring NetWare Management Agent 2.6

Configuring NLM Load Parameters . . . . .	31
Load Parameters for SERVINST.NLM . . . . .	31
Load Parameters for HOSTMIB.NLM . . . . .	32
Load Parameters for NTREND.NLM . . . . .	33
Load Parameters for FINDNMS.NLM . . . . .	35
Setting Default Trends and Thresholds . . . . .	36
Changing the Initial Trend Values . . . . .	37
Setting the Sample Interval . . . . .	38
Setting the Trend Buckets . . . . .	39
Enabling or Disabling a Trend File . . . . .	41
Backing Up Trend Data . . . . .	41
Changing the Initial Threshold Values . . . . .	41
Setting Rising and Falling Thresholds . . . . .	42
Enabling or Disabling a Threshold Trap . . . . .	43
Controlling Alarm Generation . . . . .	43
Defining the Community String . . . . .	45
Setting the Time Interval . . . . .	45
Using Masks . . . . .	45
Configuring Alarm Severity Levels . . . . .	46
Defining Recipients for SNMP Alarms . . . . .	47
Automatic Discovery Using FINDNMS.NLM . . . . .	47
Editing the TRAPTARG.CFG File Manually . . . . .	48
Configuring the ManageWise Console to Not Send SAP Packets . . . . .	49

## Index

## ***Overview of NetWare Management Agent 2.6***

The NetWare® Management Agent™ 2.6 software provides real-time server performance data and information about server alarms to network management consoles. NetWare Management Agent 2.6 completely replaces previous versions of NetWare Management Agent.

This chapter describes the main features and the major improvements offered by NetWare Management Agent 2.6. This chapter contains the following sections:

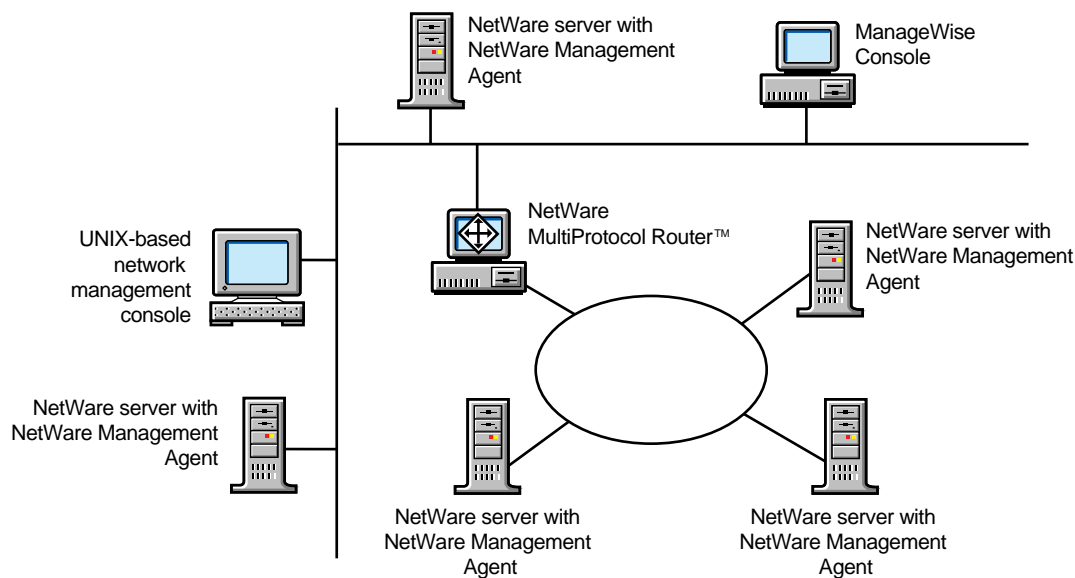
- ◆ About SNMP-Based Management
- ◆ Gathering Local Trend Information at the Server
- ◆ Support for Secure SNMP Transactions
- ◆ About NetWare Management Agent 2.6 NLM Files

## About SNMP-Based Management

The main advantage of NetWare Management Agent 2.6 is that it is based entirely on the Simple Network Management Protocol (SNMP). This makes NetWare Management Agent 2.6 easily managed by third-party management consoles as well as the ManageWise® Console. This expands the management options for using SNMP-based management consoles in conjunction with ManageWise. To facilitate this, all MIBs used with NetWare Management Agent enable you to compile at your console using any standard MIB compiler.

Figure 1-1 illustrates an internetwork using NetWare Management Agent 2.6 and two network management consoles: ManageWise and a console based on UNIX\* software.

**Figure 1-1**  
**NetWare Management Agent Configuration**



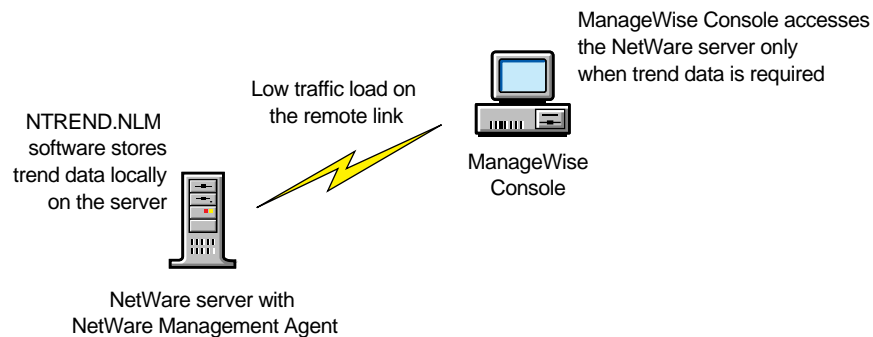
## Gathering Local Trend Information at the Server

Collecting trend data about devices creates a large amount of traffic on the network. This is because the management console must query the device continually to develop data. This can be particularly expensive

and burdensome when you are monitoring remote devices. NetWare Management Agent 2.6 provides a solution to this problem.

The NTREND.NLM software supplied with NetWare Management Agent 2.6 enables you to collect trend data at the server. Because the trend data is stored at the server, the management console does not have to poll the server constantly to maintain an internal trend data file. The management console can save on network traffic by collecting the trend data only as needed. Figure 1-2 illustrates this process using NetWare Management Agent 2.6.

**Figure 1-2**  
**Server-Based Trend Data Collection**



Refer to "Setting Default Trends and Thresholds" on page 36 for details about how to configure NTREND.NLM.

## Support for Secure SNMP Transactions

You can limit the access of management consoles performing GET and SET requests. You can accomplish this by either of the methods described in the following sections:

- ◆ “Using SNMP Over a NetWare Core Protocol Connection” on page 20
- ◆ “Setting Security for SNMP Management” on page 21

With these two methods, NetWare Management Agent 2.6 provides traditional SNMP Agent security and also provides much-enhanced security by requiring NetWare SUPERVISOR or OPERATOR login before granting access to SNMP functionality.

For details about these security features and instructions about their configurations, see Chapter 3, “Setting Up Secure SNMP Transactions.”

## About NetWare Management Agent 2.6 NLM Files

The NetWare Management Agent 2.6 software consists of the following NetWare Loadable Module™ (NLM™) files that are installed on a NetWare server.

### **SERVINST.NLM**

Implements the NetWare Server MIB (NWSERVER.MIB).

### **HOSTMIB.NLM**

Implements the standard Host Resources MIB [RFC 1514] and Novell® extensions to that MIB (NWHOSTX.MIB).

### **NTREND.NLM**

Implements the Threshold and Trend MIB (NWTREND.MIB). When loaded, NTREND.NLM sets up trends and thresholds for each monitored attribute according to the server's configuration. The NTREND.INI file contains configuration parameters for NTREND.NLM.

## NWTRAP.NLM

Implements the NetWare Server Trap MIB (NWALARM.MIB). The NWTRAP.CFG file contains configuration parameters for NWTRAP.NLM.

## FINDNMS.NLM

Used by NetWare servers running NetWare Management Agent 2.6. Employ FINDNMS.NLM to listen for ManageWise Consoles advertising themselves using the Service Advertising Protocol (SAP) number 0x026a. FINDNMS.NLM then adds the Internetwork Packet Exchange™ (IPX™) address of each ManageWise Console discovered to the list of stations that receive traps.

## NDSTRAP.NLM

Implements the NDSTRAP.MIB to capture and forward NDS™ events to SNMP management consoles.

Table 1-1 provides a brief description of the MIBs associated with NetWare Management Agent 2.6.

**Table 1-1: MIBS Provided with NetWare Management Agent 2.6**

MIB Name	Description
ndstrap.mib	This is a Novell proprietary MIB designed to capture NDS events and forward them to SNMP management consoles as SNMP TRAPS. There are at least 130 traps currently in the MIB and new ones are being added as identified.
nwalarm.mib	This is a Novell proprietary MIB that handles all the NetWare Core OS alerts and forwards them as SNMP TRAPS. It currently supports over 375 traps. New ones are being added as identified.
nwhostx.mib	This is a Novell extension to RFC1514 (the Host Resources MIB). It adds devices and components that are specific to NetWare that were not directly included in RFC1514.
nwserver.mib	This is a Novell proprietary MIB that is the basis for NetWare Core OS management. Over 300 objects are identified in this MIB. Access to the console-settable parameters for both GET and SET is defined. The MIB has several groups and tables for users, file system, volumes, queues, ODI, set parameters, and so forth.

**Table 1-1: MIBS Provided with NetWare Management Agent 2.6**

MIB Name	Description
nwtmsync.mib	This is a Novell proprietary MIB that allows for SNMP management of TIMESYNC.NLM. It provides access to the list of Time Sources as well as Time Clients. You may also access the Clock Structure through this MIB.
nwtrend.mib	This is a Novell proprietary MIB that keeps track of objects which are most useful when tracked over a period of time. Things like CPU utilization and packets received have limited value as static numbers, but when monitored at regular intervals for a period of time, they tell a lot about what is happening on a server. NTREND also provides for the setting of user definable thresholds for the managed objects and will send SNMP TRAPs when a threshold is exceeded.
rfc1514.mib	This is the Internet Standard Host Resources MIB. It defines general categories about a host machine, including physical components of the system such as disks, memory, cpu, printers, adapter cards, and so forth. It has provision for running installed software.

## 2 *Installing NetWare Management Agent 2.6*

This chapter describes the NetWare® server hardware, version, and system configuration requirements for installing NetWare Management Agent™ 2.6 software. The chapter also provides information about how to get NetWare Management Agent 2.6 up and running on NetWare 3.1x, NetWare 3.2, NetWare 4.1x, and NetWare 5™ or later servers.

Important



If you are installing ManageWise® 2.6, NetWare Management Agent 2.6 is automatically installed by default on the ManageWise server. ManageWise 2.6 allows you to install NetWare Management Agent 2.6 on multiple servers.

This chapter contains the following sections

- ◆ NetWare Server Hardware Requirements
- ◆ Versions of NetWare Supported
- ◆ Installing NetWare Management Agent on Multiple Servers
- ◆ Installing NetWare Management Agent on SFT III Servers
- ◆ Loading and Unloading NetWare Management Agent 2.6
- ◆ After Installation

## NetWare Server Hardware Requirements

The NetWare Management Agent files must be installed on a server that meets these hardware requirements:

- ◆ An additional 2 MB RAM on NetWare 3.1x servers, NetWare 3.2 servers, NetWare 4.1x, and NetWare 5 servers. For NetWare SFT III™ servers, the additional 2 MB RAM must be installed on the IO Engines and MS Engine.

At least 1 MB of memory (cache nonmovable) is required to load the NLM™ files, and at least 1 MB (alloc short term) is recommended for memory allocations.

Allocation memory requirements vary depending on the server configuration (disks, volumes, NLM files, and so forth). After you load NetWare Management Agent, verify that you have at least 40 percent of available memory resources for file caching. Unpredictable results occur when there is insufficient server memory.

- ◆ At least 4 MB of free disk space on the SYS: volume. You need 2MB to install NetWare Management Agent and another 2 MB to run NTREND files.

## Versions of NetWare Supported

Use NetWare Management Agent 2.6 only with the following versions of NetWare:

- ◆ NetWare 5, intraNetWare, NetWare 4.1x, NetWare 3.2, and NetWare 3.1x.
- ◆ NetWare SFT III, NetWare SMP, and NetWare IP.
- ◆ NetWare 4.1 for OS/2\*.

This product should *not* be used with the following versions:

- ◆ NetWare versions prior to NetWare 3.11.
- ◆ NetWare 4™ servers prior to NetWare 4.1.

## Upgrading NetWare Management Agent

If you are upgrading a manageable server, then you must reinstall the NetWare Management Agent software.



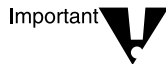
Note

If you are upgrading the network operating system, reinstall NetWare Management Agent software. Upgrade your server and then follow the instructions in the next section, "Installing the NetWare Management Agent 2.6 Software."

After you complete the installation, refer to the section "After Installation," for information on the location of the agent files.

## Installing the NetWare Management Agent 2.6 Software

If you are installing NetWare Management Agent 2.6 over previous versions, make sure that you unload all the NetWare Management Agent NLM files before you proceed with the installation.



Important

Before installing NetWare Management Agent 2.6, make sure you have updated your server with the latest software. Download the support patches from the Novell web site at <http://www.support.novell.com>.

Installation of the NetWare Management Agent software can be performed from a Windows 95\*, Windows 98, or a Windows NT\* workstation. Before installing, make sure to check the following items:

Make sure you have the following components:

- ◆ NetWare Management Agent 2.6 or ManageWise 2.6 software
- ◆ License software

The installation procedures are described in the following sections:

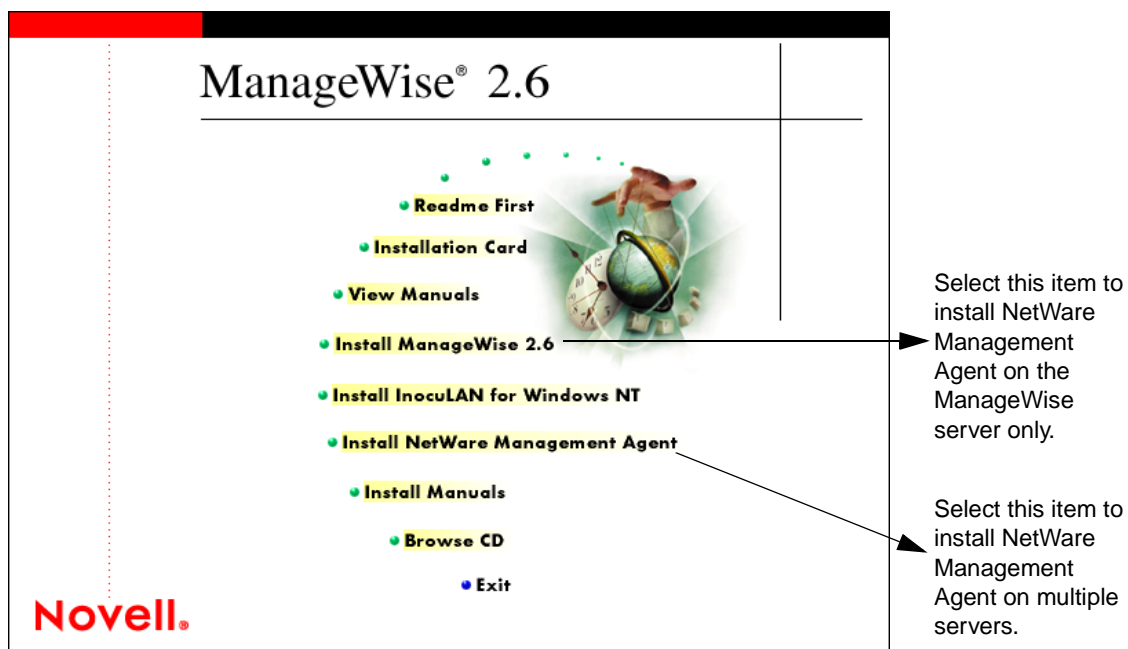
Topic	See
"Installing NetWare Management Agent on Multiple Servers"	page 10
Installing NetWare Management Agent on SFT III Servers	page 11
Installing NetWare Management Agent 2.6 from Windows	page 12

## Installing NetWare Management Agent on Multiple Servers

During the installation of ManageWise 2.6, NetWare Management Agent 2.6 is automatically installed by default on the ManageWise server. ManageWise 2.6, however, allows you to install NetWare Management Agent 2.6 on multiple servers.

To install Netware Management Agent 2.6 on multiple servers, select the *Install NetWare Management Agent* option on the ManageWise 2.6 screen as shown in Figure 2-1.

Figure 2-1  
Selecting Multiple Server Installation



To continue with the installation, go to Step 3 on page 13 under the section "Installing NetWare Management Agent 2.6 from Windows."

## Installing NetWare Management Agent on SFT III Servers

To install NetWare Management Agent 2.6 on SFT III servers, use the Windows installation procedure for the MS Engine only. To install NetWare Management Agent on the IO Engines, refer to the following section on “Updating IO Engine System and Startup Files.”



Note When you start the installation, be sure to insert the NetWare Management Agent diskette into the drive on the primary server.

For more information on installing NetWare Management Agent on the MS engine, refer to “Installing NetWare Management Agent 2.6 from Windows” on page 12.

### Updating IO Engine System and Startup Files

After you install NetWare Management Agent on the MS Engine, you must update the system and startup files for both IO Engines.

1. Update only one of the IO Engine system files. On an IO Engine, open the IO1AUTO.NCF or IO2AUTO.NCF file and add NMA2.NCF statement .
2. Open the IOSTART.NCF file on both IOEngines and type the following text:

```
Set Memory IOEngine Borrows Ahead From MEngine =  
100000
```

3. Restart the servers.

For more information on updating the files on the IO Engines, refer to the Post-Installation Help file.

### Example of NMAx.NCF file

This example shows you a list of commands in the NMA2.NCF file.

```
load findnms  
load ntrend  
load hostmib  
load nwtrap  
load servinst
```

## Restarting the SFT III Servers

The procedure for restarting SFT III servers after you install NetWare Management Agent 2.6 differs slightly from the procedure for a standard NetWare 4.1x server.

1. **Issue the following commands *on both engines*:**

**DOWN**

The server is safely brought down in orderly fashion.

**EXIT**

2. **Return to the DOS prompt and enter,**

**MSERVER**

The server starts up.

3. **When both servers are back up, issue the following command at the server console prompt of the *primary server*.**

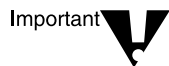
**ACTIVATE SERVER**

The two SFT III servers are synchronized.

## Installing NetWare Management Agent 2.6 from Windows

Complete the following procedure to install NetWare Management Agent 2.6 from Microsoft\* Windows—Windows 95, Windows 98, or Windows NT—on one or more selected NetWare 5, NetWare 4.1x, NetWare 3.2, or NetWare 3.1x servers.

NetWare Management Agent Setup saves all the files replaced on the server in the SYS:\NMA.SAV directory. NetWare Management Agent Setup overwrites the NWTRAP.NLM and NWTRAP.CFG files.



Before installing NetWare Management Agent, make sure you have Supervisor rights to the server (or servers), you are installing on.

To install NetWare Management Agent 2.6, complete these steps:

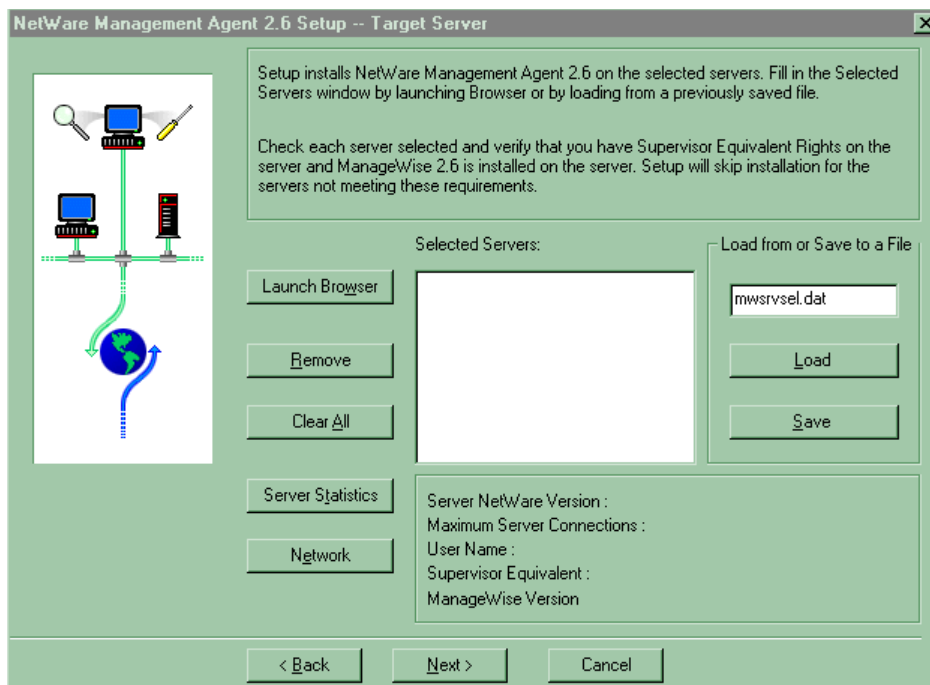
1. From Windows 95, Windows 98, or Windows NT, select **Start > Run**.

The Run dialog box appears.

2. Locate and click the **SETUP.EXE** file on your installation media.

The Setup program checks for free disk space on the ManageWise Console in the NMS directory and, if necessary, the Windows directory. If at least 3 MB of free disk space is available in either directory, the Setup program temporarily copies the NetWare Management Agent 2.6 files to the hard disk and displays the NetWare Management Agent 2.6 Setup dialog box as shown in Figure 2-2.

Figure 2-2  
Installing NetWare Management Agent

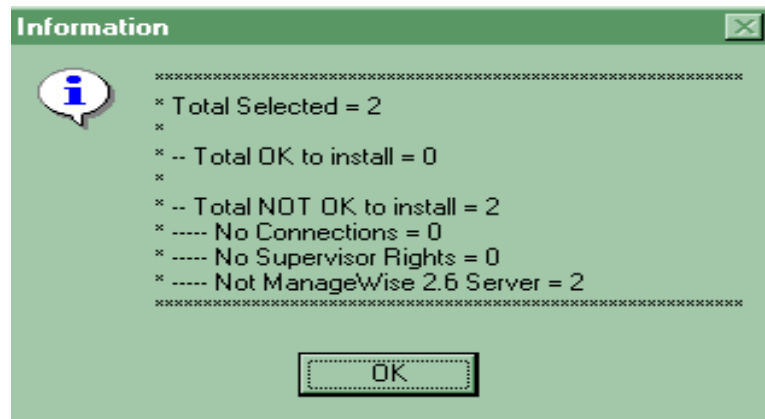


3. Click **Launch Browser** and browse the tree to select the server or servers that you want to install NetWare Management Agent.

The servers you selected are displayed in the “Selected Servers” list box.

- ◆ If you mistakenly select a server, select the server in the Selected Server list box and click *Remove*.
- ◆ If you want to remove all the selected servers from the Selected Server list box, click *Clear All*.
- ◆ To view the statistics of a server, select the server in the Selected Server list box and click *Server Statistics*. The information box shown in Figure 2-3 appears.

**Figure 2-3**  
**Server Statistics**



- ◆ You must have supervisor rights to the server where you are installing NetWare Management Agent 2.6. Click *Network* (see Figure 2-2) to log in with Supervisory rights. Enter the appropriate username and password.
- ◆ The selected servers can be saved in a file, MWSRVSEL.DAT file by clicking *Save*. Saving the selected servers in a file makes subsequent installation procedures for NetWare Management Agent 2.6 notably faster and easier.
- ◆ If you have already saved the server names in the MWSRVSEL.DAT file, then click *Load* (see Figure 2-2).

#### **4. When you have finished selecting servers, click *Next*.**

Follow the instructions on the screen and insert the License diskette, then click *OK*.



If you have a *Master License Agreement* diskette, you need to install licenses only once, regardless of how many servers you install the agent on. If you have a single-server license, you are prompted to insert the *License* diskette for each server you select.

The install program automatically replaces older files. During the installation process, the install program may discover that some files already installed are newer versions than the corresponding files on the installation diskette. Do not overwrite newer files with older versions of the files.

The installation of NetWare Management Agent 2.6 is complete.

5. Read or print the README file.
6. To launch NetWare Management Agent 2.6, bring down the server and restart it.

## Loading and Unloading NetWare Management Agent 2.6

To load NetWare Management Agent 2.6 from the server prompt, enter this command:

```
NMA5
```

To unload all the NetWare Management Agent 2.6 NLM files from the server, run the following command from the SYS:SYSTEM directory:

```
UNNMA5 .NCF
```

This concludes Chapter 2. The next chapter discusses how to set up SNMP transactions.

## After Installation

After you install NetWare Management Agent, refer to this section to find the location of the NetWare Management Agent files and NTREND data files installed. On NetWare 5 servers, the new agents are installed in the SYS:SYSTEM\NMA subdirectory and the trend log files are saved in SYS:SYSTEM\NMA\NTREND subdirectory.

## Location of the Agent Files

If the install program detects the SYS:SYSTEM\NMA directory, the NetWare Management Agent files are installed to the following directories:

- ◆ NetWare Management Agent (NMA) NLMs are installed in the SYSTEM\NMA directory.
- ◆ NMA NCF files are installed in the SYSTEM directory.
- ◆ NTREND.INI and NWTRAP.CFG are installed in the SYSTEM\NMA directory.

If the default path (SYS:\SYSTEM\NMA) is not detected on a target server, the install program installs the agent files in the following directories:

- ◆ NetWare Management Agent (NMA) NLMs are installed in the SYSTEM directory.
- ◆ NMA NCF files are installed in the SYSTEM directory.
- ◆ NTREND.INI and NWTRAP.CFG are installed in the ETC directory.

## NTREND Data Files

The Setup program does not overwrite any existing NTREND data. The existing NTREND data files are retained for use by NetWare Management Agent 2.6.

The NTREND directory stores the NTREND data files (.NT). The NTREND.NLM file uses NTREND subdirectory in the directory from which it is loaded as the default NTREND directory. After the NetWare Management Agent is installed, the first time that the NTREND.NLM file is loaded it looks for existing NTREND data (.NT) files in the NTREND directory. If the NTREND directory does not exist, it creates a subdirectory called NTREND in the directory from which it is loaded. If the NTREND data files (.NT) are stored in a different location you can direct the NTREND.NLM file to another location by modifying the LOAD NTREND statement in the NMAx.NCF file.

To edit the NMAx.NCF file:

1. Open the NMAx.NCF file with a text editor.
2. Locate the LOAD NTREND statement.
3. Add DIRECTORY=<pathname> parameter. For example,

```
LOAD NTREND DIRECTORY=SYS:\NTREND
```

4. Save the NMAx.NCF file and reload it.

The setup program installs the NMAx.NCF file with following LOAD NTREND statement:

- ◆ If the existing NMAx.NCF file has the LOAD NTREND statement with the DIRECTORY=<pathname> parameter included in it, the setup program uses the same pathname.
- ◆ If the NTREND.NLM file is installed in SYSTEM directory and SYS:\SYSTEM\NTREND directory does not exist and SYS:\NTREND directory exists, the LOAD NTREND statement includes the DIRECTORY=SYS:\NTREND parameter.

Otherwise, the LOAD NTREND statement will not include the DIRECTORY= parameter. If you wish to direct the NTREND.NLM file to use another location for the NTREND data files, use the above steps to edit the NMAx.NCF file to include the DIRECTORY=<pathname> parameter to the LOAD NTREND statement.



## **3** ***Setting Up Secure SNMP Transactions***

Because NetWare Management Agent 2.6 software is based on SNMP, all actions that are directed from network management consoles to a server involve SNMP SET and GET commands. Any console action that gets data from the server does so by issuing an SNMP GET command. An SNMP SET command is required to set server alarm thresholds or configuration parameters. In most cases, you are unaware of the underlying SNMP commands required to carry out requests you make from a management console.

Conducting these management operations from a remote management console, such as the ManageWise Console, raises the problem of ensuring security. In particular, if unchecked, unauthorized users setting configuration parameters on a server could cause severe performance problems or even sabotage network operations.

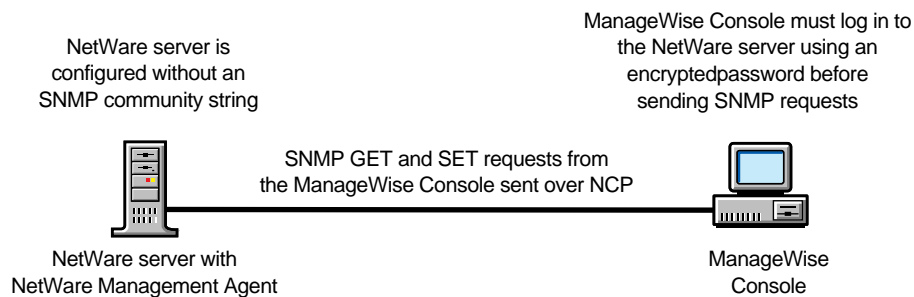
For these reasons, NetWare Management Agent 2.6 provides security for SNMP commands through mechanisms described later in this chapter.

## Using SNMP Over a NetWare Core Protocol Connection

NetWare Management Agent 2.6 provides maximum security using the NetWare Core Protocol™ (NCP™) option. When configured this way, a NetWare server accepts only SNMP SET or GET commands from management consoles that log in to the NetWare server with SUPERVISOR or OPERATOR privileges.

In this configuration, the NetWare server accepts SET and GET commands from appropriately logged-in consoles and ignores whatever SNMP community string might be used in the command. Because the login password is encrypted, this password is secure from anyone using a network protocol analyzer to decode packets on the network. Figure 3-1 illustrates this configuration.

**Figure 3-1**  
**Server Configuration with SNMP Over NCP**



You can configure the SNMP SET and SNMP GET commands separately. For example, you might want to allow open access to configuration information on your server, but allow only limited access for changing configuration parameters. In this situation, you would configure the server to allow only SNMP SET transactions over NCP.

You set this option at the NetWare server using either LOAD SNMP command, as described in “Configuring Community Name Options Using SNMP LOAD Commands” on page 24. You can also set this option using the Internetworking Configuration utility (INETCFG) on NetWare 4.x or NetWare 5.x servers or servers running NetWare MultiProtocol Router software, as described in “Configuring Community Name Options Using INETCFG” on page 25.

To configure a ManageWise Console to operate with a NetWare server using this configuration, see “Setting Up the ManageWise Console for Secure SNMP Transactions” on page 28.



Note NCP cannot be used on SFT III™ server IOEngines. Therefore, you must set the ControlCommunity string on the IOEngine to the community name the MEngine uses.

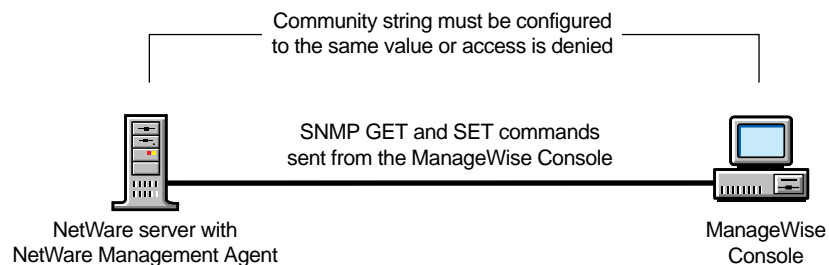
## Setting Security for SNMP Management

Security for SNMP management is often provided through use of the SNMP community name. NetWare Management Agent 2.6 provides this mechanism that enables you to limit the access of management consoles performing GET and SET commands.

To accomplish this, set a unique community name at the NetWare server where NetWare Management Agent 2.6 is installed. Any console requesting access to that server must use the same community name or access is denied.

Figure 3-2 illustrates the concept of community name-based security using the ManageWise Console.

**Figure 3-2**  
**Secure SNMP**  
**Commands Using**  
**the Community**  
**Name**



This security mechanism is limited and insufficient for networks where security is highly valued. This is because the community name is not encrypted and can be read easily using a network protocol analyzer.

See “Configuring Security Options on a NetWare Server” on page 23 for configuration instructions. To configure a ManageWise Console to

operate with a NetWare server in this configuration, see “Setting Up the ManageWise Console for Secure SNMP Transactions” on page 28.

## **Allowing Access to a ManageWise Console and a Third-Party Management Console**

In some networks, you might want to allow access to both a ManageWise Console and a third-party network management console. In this case, only management consoles using NCP, of which the ManageWise Console is one, can operate with SNMP over an NCP connection. In this situation, more security than is typically provided by community name access can be made available.

You can accomplish this by setting the community name at the ManageWise Console to a different value than the value that is set at the server and by setting up the ManageWise Console to provide SNMP over NCP connectivity.

In this configuration, the ManageWise Console always logs in to the NetWare server with SUPERVISOR or OPERATOR privileges when conducting an SNMP command. Although the ManageWise Console uses an incorrect or null community name, it succeeds in logging in because the NetWare server ignores the community name for consoles that have logged in with SUPERVISOR or OPERATOR privileges. If someone monitors any of these commands using a network protocol analyzer, they obtain an incorrect community name.

Because the NetWare server has not been configured for exclusive SNMP access to users with SUPERVISOR or OPERATOR privileges, any SNMP command that contains the correct community name is accepted. A third-party console can perform SNMP commands on this server by using the correct community name in the command.

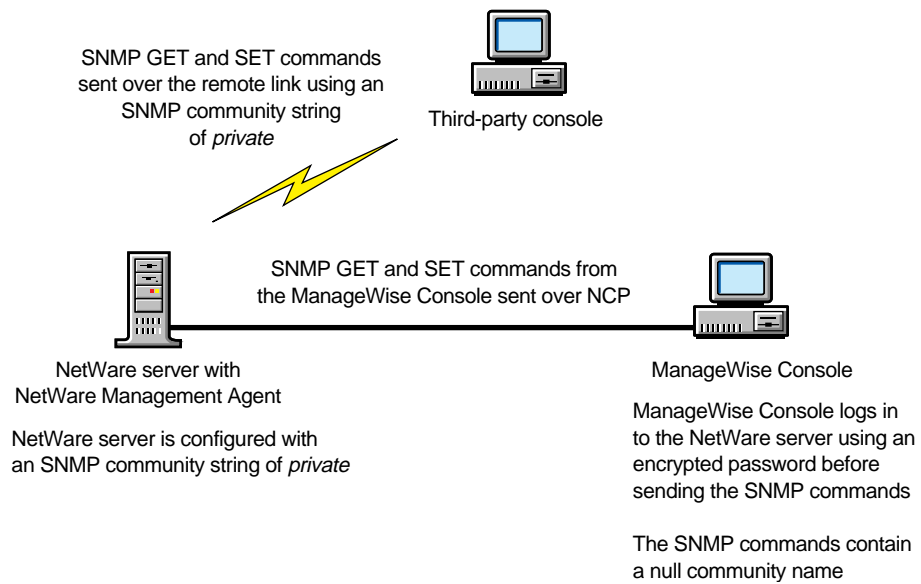
These commands can be monitored and decoded using a network protocol analyzer. From this decoding, the correct community name can be deciphered and used to breach the security of the server. Additional security is provided, however, because only the commands conducted by the third-party console can be deciphered.

This configuration is most useful for network management configurations that use ManageWise for local management of a

NetWare server but also allow occasional management from a third-party management console at a remote site.

Figure 3-3 illustrates this type of NetWare Management Agent 2.6 configuration.

**Figure 3-3**  
**Secure SNMP Transaction Using a False Community Name**



Refer to the next section for configuration instructions. To configure a ManageWise Console to operate with a NetWare server in this configuration, refer to “Setting Up the ManageWise Console for Secure SNMP Transactions” on page 28.

## Configuring Security Options on a NetWare Server

Configuring security on a NetWare Management Agent 2.6 server involves setting the *SNMP community name*. You configure security access for SNMP transactions using either SNMP LOAD command-line parameters (NetWare 3™ servers, NetWare 4™ servers, or NetWare 5™ servers) or through INETCFG (NetWare 4.x servers, NetWare 5.x

servers, or servers with NetWare MultiProtocol Router™ software installed).

Community names are used to authenticate SNMP commands received at the NetWare Management Agent 2.6 server. The community name in a message requesting a given access type must match the name defined by that access type by one of the SNMP community options.

Community names are arbitrary ASCII strings of up to 64 characters. They can include any character except space, tab, open square bracket ([), equal sign (=), colon (:), semicolon (;), and number sign (#).

The community name can be set to any of the following options:

- ◆ Read access or read/write access by anyone
- ◆ Read access or read/write access by consoles specifying the correct community name
- ◆ Read access or read/write access by users with SUPERVISOR or OPERATOR privileges only

## Configuring Community Name Options Using SNMP LOAD Commands

The LOAD command accepts the following SNMP option parameters:

- ◆ *MonitorCommunity*—Sets the community name for read-only (GET) access. The default value is *public*. The syntax is as follows:

```
LOAD SNMP MonitorCommunity=community name
```

- ◆ *ControlCommunity*—Sets the community name for read and write (GET and SET) access. By default, this community name is disabled.

When *ControlCommunity* is disabled, write access is available only to users who log in with SUPERVISOR or OPERATOR privileges.

The syntax is as follows:

```
LOAD SNMP ControlCommunity=community name
```

These options set the community name for the indicated community. Community names are case-sensitive.

Table 3-1 shows examples of available settings.

**Table 3-1**  
**SNMP Example Settings**

Access available to requester with	Read Only	Read/Write
Any community name	LOAD SNMP MonitorCommunity= or LOAD SNMP ControlCommunity=	LOAD SNMP ControlCommunity=
Community name: "secret"	LOAD SNMP MonitorCommunity= <i>secret</i> or LOAD SNMP ControlCommunity= <i>secret</i>	LOAD SNMP ControlCommunity= <i>secret</i>
Community name: "str1" or "str2"	LOAD SNMP MonitorCommunity= <i>str1</i> and LOAD SNMP ControlCommunity= <i>str2</i>	
SUPERVISOR or OPERATOR	LOAD SNMP MonitorCommunity and LOAD SNMP ControlCommunity	LOAD SNMP ControlCommunity

## Configuring Community Name Options Using INETCFG

To configure the community name options using INETCFG, follow these steps:

Procedure

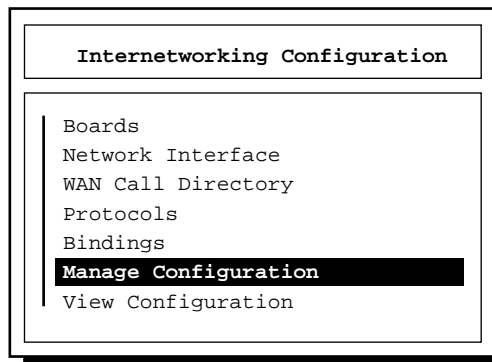


1. At the server prompt, enter the following command:

```
LOAD INETCFG
```

The Internetworking Configuration menu is displayed.

**Figure 3-4**  
**Internetworking**  
**Configuration Menu**



- 2. From the Internetworking Configuration menu, select *Manage Configuration*.**

The Manage Configuration menu is displayed.

- 3. Select *Configure SNMP Parameters*.**

The SNMP Parameters menu is displayed.

- 4. Select *Monitor State*.**

- 5. Select one of the following options, and then press Enter.**

These options let you indicate how SNMP handles SNMP read operations coming from outside this server.

Option	Description
Any Community May Read	Allows all GET (read) commands no matter what community name is provided in the incoming read request.
Leave as Default Setting	Avoids changing the Monitor Community name from its default (which is usually <i>public</i> ). The default Monitor Community can still be changed manually through SNMP command-line options, as described in "Configuring Community Name Options Using SNMP LOAD Commands" on page 24.
No Community May Read	Allows GET (read) commands only for requests that are made by management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community name provided in an incoming read request is ignored.

Option	Description
Specified Community May Read	<p>Allows only GET (read) commands for requests that contain the name specified in the Monitor Community field.</p> <p>If you selected this option, enter a name in the Monitor Community field, and then press Enter.</p> <p>Enter the name of the community that is allowed to read management information. SNMP management stations that belong to this community can read the network management database.</p>

**6. Select *Control State*.**

**7. Select one of the following options, and then press Enter.**

These options allow you to indicate how SNMP handles SNMP write operations coming from outside this server:

Option	Description
Any Community May Write	Allows all SET (write) commands, no matter what community name is provided in the incoming write request.
Leave as Default Setting	Avoids changing the Control Community from its default, which is usually to allow write requests only for management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. You can change the default manually through SNMP command-line options, as described in "Configuring Community Name Options Using SNMP LOAD Commands" on page 24.
No Community May Write	Allows SET (write) commands only for requests that are made by management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community name provided in an incoming write request is ignored.
Specified Community May Write	Allows SET (write) commands only for requests that are made by management consoles that have logged in to the server with SUPERVISOR or OPERATOR privileges. Any community name provided in an incoming write request is ignored.

**8. When you are finished, press Esc. If prompted, select *Yes* to save changes to the SNMP parameters, and then press Enter.**

The Manage Configuration menu is displayed.

9. To return to the Internetworking Configuration menu, press Esc.

10. To exit INETCFG, press Esc.

Note



Changes made in INETCFG are not active immediately. To put these changes into effect, bring down the server and restart it.

## Setting Up the ManageWise Console for Secure SNMP Transactions

Configuring secure SNMP transactions involves setting parameters at both the console and the server being managed. This section describes how to configure a ManageWise Console for each of the following SNMP security options:

- ◆ Configuring the SNMP community string for SET and GET commands
- ◆ Directing the ManageWise Console to log in with SUPERVISOR or OPERATOR privileges for SNMP SET and GET commands

To configure the ManageWise Console SNMP security options, follow these steps:

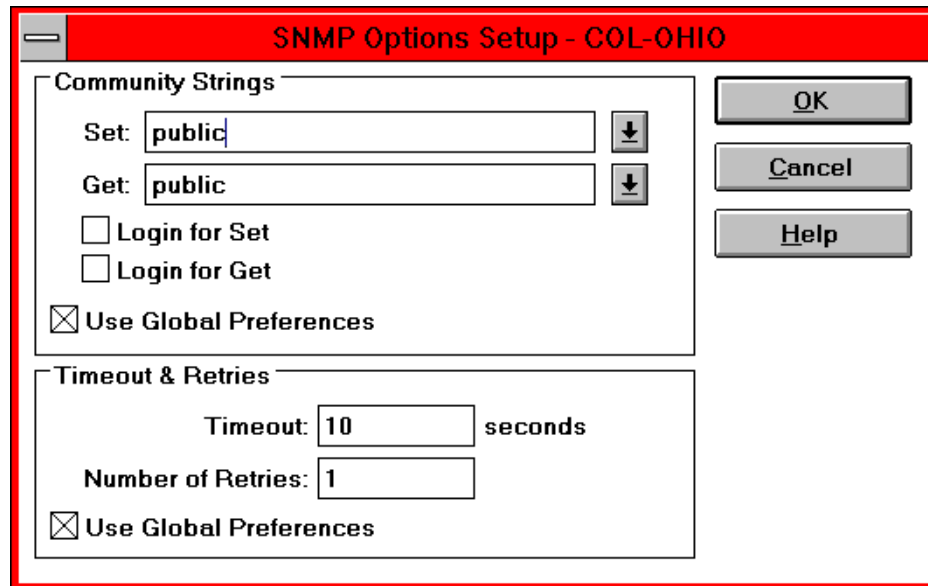
Procedure



1. **Select a ManageWise Server.**
2. **Select *Configure > SNMP Options*.**

The SNMP Options Setup dialog box is displayed as shown in Figure 3-5.

Figure 3-5  
SNMP Setup Options



The image shows a dialog box titled "SNMP Options Setup - COL-OHIO". It is divided into two main sections: "Community Strings" and "Timeout & Retries".

**Community Strings section:**

- Set:  (with a dropdown arrow)
- Get:  (with a dropdown arrow)
- ☐ Login for Set
- ☐ Login for Get
- ☒ Use Global Preferences

**Timeout & Retries section:**

- Timeout:  seconds
- Number of Retries:
- ☒ Use Global Preferences

On the right side of the dialog box, there are three buttons: "OK", "Cancel", and "Help".

3. If you want the ManageWise Console to log in with **SUPERVISOR** or **OPERATOR** privileges, select the following options:
  - ◆ For SET (write) commands, select the Login for SET check box. The server ignores SET community name in this case.
  - ◆ For GET (read) commands, select the Login for GET check box. The server ignores GET community name in this case.
4. Otherwise, select the following options:
  - ◆ Select a community string for SNMP SET commands.

You can either accept the default value of *public*, type a unique value for the server you are managing, or select *null* for no community string value.
  - ◆ Select a community string for SNMP GET commands.

You can either accept the default value of *public*, type a unique value for the server you are managing, or select *null* for no community string value.

5. When you are finished, click OK to exit the SNMP Options Setup dialog box and set the new values.

## 4 **Configuring NetWare Management Agent 2.6**

Once NetWare Management Agent 2.6 software has been installed on your system, it is ready to operate in its default state. In most cases, this configuration is sufficient; however, you can customize NetWare Management Agent 2.6.

Examine each of the configuration options in the sections that follow to determine whether you require any of the functionality provided.

### **Configuring NLM Load Parameters**

The NetWare Management Agent 2.6 installation process creates the NMA2.NCF file in the SYS:\SYSTEM directory. When the NetWare server is started, this file automatically loads all the NLM files required for NetWare Management Agent 2.6 in a default configuration state. There are, however, several LOAD parameters that you can configure for each of the NLM files used with the agent.

You can configure your server to use these options by editing the NMA2.NCF file on your server. Also, if your server is already running, you can unload any of these NLM files and then load them at the NetWare server console using any of the configuration parameters. You can configure these parameters at the NetWare server console or by using the NetWare remote console utility, RCONSOLE.

The sections that follow describe each of the command-line parameters that you can configure for NetWare Management Agent 2.6.

#### **Load Parameters for SERVINST.NLM**

SERVINST.NLM implements the NetWare Server MIB (NWSERVER.MIB). You can load SERVINST.NLM at the command line with any or all of the following parameters:

**LOAD SERVINST D U=*n* V B=*n* H**

Parameter	Description
D	<p>DisableSets—If this parameter is present, SERVINST.NLM does not allow SNMP SET commands for objects in NWSERVER.MIB.</p> <p>Default: SETS enabled (subject to SNMP security)</p>
U= <i>n</i>	<p>UpdateInterval=<i>n</i>—Sets the list update interval to <i>n</i> (<i>n</i> is a value in seconds). This determines how often certain internal lists kept by SERVINST.NLM (such as volumes and queues) are updated. Set this parameter higher, to minimize the number of CPU cycles used by SERVINST.NLM, or lower, to guarantee immediate reporting of server status changes that affect the lists.</p> <p>Default: 300 seconds.</p>
V	<p>Verbose—Displays informational messages.</p> <p>Default: Off.</p>
B= <i>n</i>	<p>BuildUserListHour=<i>n</i>—The local time each day on a 24-hour clock (0 to 23) at which the SERVINST.NLM software builds a list of users that have access to the server.</p> <p>Default: 2 (2:00 AM).</p>
H	<p>Help—Displays help on command-line parameters. If you use the H parameter, SERVINST.NLM displays the help messages and then exits. It does not remain loaded even if other parameters are entered on the command line.</p>

## Load Parameters for HOSTMIB.NLM

HOSTMIB.NLM implements both the standard Host Resources MIB [RFC 1514] and Novell's extensions to the Host Resources MIB (NWHOSTX.MIB). You can load HOSTMIB.NLM at the command line with any or all of the following parameters:

LOAD HOSTMIB.NLM D U=*n* V H

Parameter	Description
D	<p>DisableSets—If this parameter is present, HOSTMIB does not allow SNMP SET commands for objects in RFC1514.MIB or NWHOSTX.MIB.</p> <p>Default: SETS enabled (subject to SNMP security).</p>
U= <i>n</i>	<p>UpdateInterval=<i>n</i>—Sets the list update interval to <i>n</i> (<i>n</i> is a value in seconds). This determines how often certain internal lists kept by HOSTMIB.NLM are updated. Set this parameter higher, to minimize the number of CPU cycles used by HOSTMIB.NLM, or lower, to guarantee immediate reporting of server status changes that affect the lists.</p> <p>Default: 60 seconds.</p>
V	<p>Verbose—Displays informational messages.</p> <p>Default: Off.</p>
H	<p>Help—Displays help on command-line parameters.</p> <p>Default: Off.</p>

## Load Parameters for NTREND.NLM

NTREND.NLM implements the Threshold and Trend MIB (NWTREND.MIB).

When first loaded, NTREND.NLM automatically sets up trends and thresholds for each monitored attribute according to the server's configuration from values stored in the NTREND.INI file (located in the SYS:\ETC directory). You can edit this file as described in "Setting Default Trends and Thresholds" on page 36.

Thereafter, as configuration changes occur over time, NTREND.NLM adjusts to changes in the number and type of physical network interfaces, queues, volumes, and disks. Default thresholds are set only for important parameters. The user can later use SNMP SET commands to set thresholds for parameters like files read and packets in.

A trend file is created for each monitored attribute instance, even if trending is disabled for that object. The file header contains all the information from `nwtControlTableEntry`, and the rest of the file stores the sample history (if any). Once a trend file is created, it exists until deleted explicitly by the operator, even if the monitored object (queue, for example) no longer exists. When a monitored object no longer exists, the associated `nwtControlStatus` is recorded as invalid.

You can load `NTREND.NLM` at the command line with any or all of the following parameters:

**LOAD NTREND D=<dir> R V H**

Parameter	Description
D= <dir>	<p>Directory=&lt;dir&gt;—Enables you to specify the volume and directory where <code>NTREND.NLM</code> stores the history data files. Example: To use <code>VOL1: \TEST</code> as the directory for trending files, enter the following command:</p> <pre>LOAD NTREND D=VOL1: \TEST</pre> <p>Default: <code>SYS:\NTREND</code>.</p>
R	Reset—Causes <code>NTREND.NLM</code> to discard all the old trending history data and restart the sampling.
V	<p>Verbose—Displays informational messages.</p> <p>Default: Off.</p>
H	<p>Help—Displays help on command-line parameters.</p> <p>Default: Off.</p>

## Load Parameters for FINDNMS.NLM

FINDNMS.NLM discovers workstations running the ManageWise Console by reading its server's bindery and looking for SAP 0x026a, which is broadcast periodically by ManageWise. FINDNMS.NLM then adds the IPX address of the console to the list of stations that want to receive traps. Entries that cease to send SAP packets are removed from the list at an interval set by the aging-period parameter.

Third-party management stations using SNMP over IPX can share this mechanism by broadcasting SAP 0x026a periodically, or they can use the TRAPTARG.CFG method described in "Defining Recipients for SNMP Alarms" on page 47. You can load FINDNMS.NLM at the command line with any or all of the following parameters.

**LOAD FINDNMS U=*n* A=*n* H**

Parameter	Description
U= <i>n</i>	UpdateInterval= <i>n</i> —Interval, in seconds, between reads by FINDNMS.NLM of the server's bindery.  Default: 300 (5 minutes).
A= <i>n</i>	AgingPeriod= <i>n</i> —Period, in seconds, to wait before removing stations that have ceased to send SAP packets from the table created by FINDNMS.NLM.  Default: 600 (10 minutes).
H	Help—Displays help on command-line parameters.  Default: Off.

## Setting Default Trends and Thresholds

When NTREND.NLM is first loaded, it obtains the initial (default) values for trends and thresholds from the NTREND.INI file. This file is stored in the NetWare server's SYS:\ETC directory. The initial values in the NTREND.INI file are also used whenever a new trend file is created. A new trend file is created when an instance of a monitored object (volume, disk, interface, and so on) is discovered on the server. Example 4-1 presents a portion of a sample NTREND.INI file.

**Example 4-1**  
**Sample NTREND.INI File**

#-----								
#	Sample	Trend	Threshold					
# Parameter	Interval	Buckets	Enbl	Rising	Falling	Enbl	Type	
#-----								
NUMBER_LOGGED_IN_USERS	5	60	1	100	90	1	rising	
NUMBER_LOGGED_IN_USERS	7	8928	1	90	81	1	rising	
NUMBER_CONNECTIONS	5	60	1	0	0	0	rising	
NUMBER_CONNECTIONS	7	8928	1	0	0	0	rising	
FILE_READS	5	60	1	0	0	0	rising	
FILE_READS	7	8928	1	0	0	0	rising	
FILE_WRITES	5	60	1	0	0	0	rising	
FILE_WRITES	7	8928	1	0	0	0	rising	
FILE_READ_KBYTES	5	60	1	0	0	0	rising	
FILE_READ_KBYTES	7	8928	1	0	0	0	rising	
FILE_WRITE_KBYTES	5	60	1	0	0	0	rising	
FILE_WRITE_KBYTES	7	8928	1	0	0	0	rising	
LSL_IN_PACKETS	5	60	1	0	0	0	rising	
LSL_IN_PACKETS	7	8928	1	0	0	0	rising	
LSL_OUT_PACKETS	5	60	1	0	0	0	rising	
LSL_OUT_PACKETS	7	8928	1	0	0	0	rising	
NCP_REQUESTS	5	60	1	0	0	0	rising	
NCP_REQUESTS	7	8928	1	0	0	0	rising	
CPU_UTILIZATION	5	60	1	90	81	1	rising	
CPU_UTILIZATION	7	8928	1	80	72	1	rising	
CACHE_BUFFERS	5	60	1	45	40	1	falling	
CACHE_BUFFERS	7	8928	1	0	0	1	falling	
CODE_DATA_MEMORY	5	60	1	0	0	0	rising	
CODE_DATA_MEMORY	7	8928	1	0	0	0	rising	

Once the NTREND.NLM software is running, trend and threshold values can be changed (using the ManageWise Console) by making use of the threshold-setting features of ManageWise. If the server is brought down, it retains the last trend and threshold settings that were set. A NetWare server with NetWare Management Agent 2.6 installed only returns to the initial values of the NTREND.INI file when any of the following situations occurs:

- ◆ NTREND.NLM is loaded for the first time.
- ◆ NTREND.NLM is loaded with the Reset argument.
- ◆ NTREND.NLM is loaded with the Directory argument and the specified directory does not already contain the trend files.
- ◆ Trend files have been deleted manually.
- ◆ If a system administrator changes the server configuration by adding a new volume, disk, interface, and so on, the trend value of the new device is set to the default value.



Trends are not maintained for CD-ROM volumes. Therefore, changing trend parameters for CD-ROM volumes has no effect.

You can edit the NTREND.INI file to change the initial trend and threshold values of the NTREND.NLM software, as described in the sections that follow.

## Changing the Initial Trend Values

The trend values in the NTREND.INI file specify the time interval (Sample Interval) at which a particular trend parameter is sampled, the duration of time for which those samples are kept (Trend Buckets), and whether this sampling parameter is enabled (Enbl). For each value specified by a line in the NTREND.INI file, a trend record is stored in a separate file in the SYS:\NTREND directory by default.

Example 4-2 is an example of a line in the NTREND.INI file for the NUMBER\_LOGGED\_IN\_USERS trend parameter with a Sample Interval of 5, Trend Buckets specified at 60, and the enable parameter specified at 1 (enabled).

**Example 4-2**  
**Sample Trend Values**

```
#-----
# Parameter      | Sample   | Trend   |          | Threshold |          |
#                 | Interval | Buckets | Enbl    | Rising    | Falling  | Enbl    | Type
#-----
NUMBER_LOGGED_IN_USERS 5          60      1      100      90      1      rising
```

The sections that follow describe how to set or alter each of the parameters required for a trend file.

You can specify more than one sampling interval or duration for any trend parameter by creating another line in the NTREND.INI file. In the sample file in Example 4-1, two time intervals and durations are sampled for each parameter.

### Setting the Sample Interval

The NTREND.NLM software enables you to collect samples of a specified parameter at any of 12 possible time intervals (Sample Interval), from 5 seconds to 1 day.

Each of these Sample Intervals is specified by a code number in the NTREND.INI file. Table 4-1 specifies the code used in the NTREND.INI file for each of the Sample Intervals permitted. For example, if you want to sample a particular trend parameter once every hour, you would use the code 9.

**Table 4-1**  
**Time Interval Code**

Sample Interval	Code
5 seconds	1
10 seconds	2
15 seconds	3

**Table 4-1** *continued*  
**Time Interval Code**

Sample Interval	Code
30 seconds	4
1 minute	5
5 minutes	6
15 minutes	7
30 minutes	8
1 hour	9
4 hours	10
8 hours	11
1 day	12

### Setting the Trend Buckets

Once you have determined a Sample Interval for collecting samples, you must set a duration of time for which you want to collect samples. For example, if you selected a Sample Interval of one hour for a particular parameter, you might decide that you want to be able to review the state of that parameter for every hour over the duration of a day.

You determine the duration of time for which a parameter is collected by the number of Trend Buckets you specify. You must specify a Trend Bucket for each sample that is collected over a specific period of time. For example, to review the state every hour for 1 day, 24 Trend Buckets (1 per hour x 24 hours in a day) are required.

The number of Trend Buckets required for any particular Time Duration and Sample Interval is calculated easily. However, for your convenience, Table 4-2 shows the number of Trend Buckets required for each Sample Interval allowed, for each of seven possible time durations of from 1 hour to 1 year.

Once the Sample Interval and the Time Duration for trend collection is set, you can compute the size of trend files. The number of Trend Buckets possible, and the approximate size in kilobytes (in

parentheses), for a given Sample Interval and Time Duration are given in Table 4-2. The size of each Trend Bucket is 4 bytes plus 512 bytes for the header file. For example, if the sampling interval is 5 seconds for a period of 1 hour, the file size would be 720 Trend Buckets x 4 bytes long (rounded to the closest 4 KB boundary) plus 512 bytes for a total of 4.5 KB. There are always as many trend files (.NT) as there are enabled trends.

**Table 4-2**  
**Trend Buckets Required for Several Possible Durations**

Sample Interval	1-Hour Duration	1-Day Duration	1-Week Duration	1-Month Duration	3-Month Duration	6-Month Duration	1-Year Duration
5 seconds (KB)	720 (4)	17280 (72)	120960 (488)	535680 (2144)	1607040 (6432)	3214080 (12860)	63076400 (252308)
10 seconds (KB)	360 (4)	8640 (36)	60480 (244)	267840 (1072)	803520 (3216)	1607040 (6432)	3153600 (12616)
15 seconds (KB)	240 (4)	5760 (24)	40320 (164)	178560 (716)	535680 (2144)	1071360 (4284)	2102400 (8412)
30 seconds (KB)	120 (4)	2880 (16)	20160 (84)	89280 (360)	267840 (1072)	535680 (2144)	1051200 (4208)
1 minute (KB)	60 (4)	1440 (8)	10080 (44)	44640 (180)	133920 (540)	267840 (1072)	525600 (2104)
5 minutes (KB)	12 (4)	288 (4)	2016 (12)	8928 (40)	26784 (108)	53568 (216)	105120 (424)
15 minutes (KB)	4 (4)	96 (4)	672 (4)	2976 (16)	8928 (40)	17856 (72)	35040 (144)
30 minutes (KB)	2 (4)	48 (4)	336 (4)	1488 (8)	4464 (20)	8928 (40)	17520 (72)
1 hour (KB)	1 (4)	24 (4)	168 (4)	744 (4)	2232 (12)	4464 (20)	8760 (36)
4 hours (KB)		6 (4)	42 (4)	186 (4)	558 (4)	1116 (8)	2190 (12)
8 hours (KB)		3 (4)	21 (4)	93 (4)	279 (4)	558 (4)	1095 (8)

Table 4-2 *continued*

### Trend Buckets Required for Several Possible Durations

Sample Interval	1-Hour Duration	1-Day Duration	1-Week Duration	1-Month Duration	3-Month Duration	6-Month Duration	1-Year Duration
1 day (KB)		1 (4)	7 (4)	31 (4)	93 (4)	186 (4)	365 (4)

Once a particular time duration is exceeded for a file (all the Trend Buckets have been filled), NTREND.NLM keeps adding the most recent sample by overwriting the oldest. This means that the file contains the most recent duration recorded. For example, if you select a Sample Interval of 1 hour for a duration of 24 hours (using 24 Trend Buckets), the associated file contains the trend data for the last 24 hours.

### Enabling or Disabling a Trend File

Each line in the NTREND.INI file contains a parameter that either enables or disables the NTREND.NLM software to begin creating a trend file at startup. The total number of trend files is equal to the number of lines in the NTREND.INI file. To enable the collection of data for a trend file, set this parameter to 1. To disable the collection of data for a trend file at startup, set this parameter to 0.

### Backing Up Trend Data

Trend data is not automatically backed up. If you feel the need to back up this data, please do so manually.

### Changing the Initial Threshold Values

The default threshold values in the NTREND.INI file specify when a trap is generated. User-defined values are stored in the trend file (.NT) header. If the parameter rises above or falls below the set threshold value, a rising or falling trap type is sent. Example 4-3 is an example of a line in the NTREND.INI file for the NUMBER\_LOGGED\_IN\_USERS Trend Parameter with a Threshold Range of 90 percent to 100 percent. This implies that the threshold is 100 percent, while the lower marker is

90 percent. In Example 4-3, the falling threshold indicates the lower marker.

#### Example 4-3 Sample Trend Values

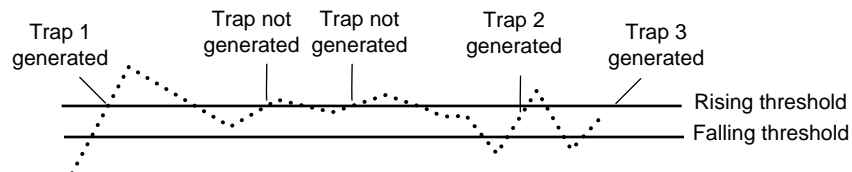
```
#-----
# Parameter      | Sample Interval | Trend Buckets Enbl | Rising Threshold Falling Enbl Type |
#-----
NUMBER_LOGGED_IN_USERS 5          60          1    100          90      1    rising
```

The sections that follow describe how to set or alter each of the parameters required for a threshold value.

### Setting Rising and Falling Thresholds

Each line in the NTREND.INI file contains a parameter for the Rising Threshold and the Falling Threshold. For each Sample Interval, a rising or falling trap can be generated as specified. After a trap is generated, another such trap is not generated until the sampled value falls below this threshold and reaches the falling threshold. Figure 4-1 provides an example of this process for a Rising Threshold trap.

Figure 4-1  
Rising Threshold



In this example, Trap 1 is generated because it is the first time that the parameter value rises above the Rising Threshold. The next two times the parameter value rises above the Rising Threshold, a trap is not generated because the parameter did not fall below the Falling Threshold. Trap 2 and Trap 3 are generated because the parameter value dropped below the Falling Threshold before exceeding the Rising Threshold.

In Example 4-3, a Rising Trap is generated the first time that the `NUMBER_LOGGED_IN_USERS` parameter exceeds the Rising Threshold value of 100. For a second Rising Trap to be generated, the parameter must fall below the Falling-Threshold of 90, and then exceed the Rising Threshold of 100 again.

### Enabling or Disabling a Threshold Trap

Each line in the `NTREND.INI` file contains a parameter that enables or disables the `NTREND.NLM` software to send traps as determined by the Rising and Falling Thresholds. This parameter is set to 1 to enable the software to send a trap for the values given, or to 0 to disable the software from sending a trap for this parameter.

## Controlling Alarm Generation

The `NWTRAP.NLM` configuration file is `NWTRAP.CFG`, which is stored in the `SYS:\ETC` directory. The configuration file is read only when `NWTRAP.NLM` is loaded; therefore, any changes made to the file do not take effect until the next time you load `NWTRAP.NLM`.



Note

On a NetWare 3.1x server, `EDIT.NLM` does not have a large enough buffer to edit the `NWTRAP.CFG` file. To edit the `NWTRAP.CFG` file, map a drive to the server `SYS:` volume and proceed from there.

You can use the `NWTRAP.NLM` configuration file to configure or change any of the following:

- ◆ Types of alarms `NWTRAP.NLM` forwards to management stations, including ManageWise.
- ◆ Community strings `NWTRAP.NLM` uses.
- ◆ Time interval during which `NWTRAP.NLM` ignores duplicate alarms.
- ◆ List of traps to be disabled, using the *mask* keyword.
- ◆ Minimum severity of alarms `NWTRAP.NLM` forwards to the management station.
- ◆ Specific alarms that you want to prevent `NWTRAP.NLM` from forwarding.

The configuration file consists of keywords and their associated data (case is ignored). Each keyword must be on a line by itself (except for mask values, where they might span several lines), and must be followed by one or more lines of associated data. Keywords are *community*, *time interval*, *mask*, and *severity*.

You can place comments anywhere in the file, even between a keyword and its associated information. A comment starts with a number sign (#), and continues to the end of the line.

Example 4-4 is an example of an NWTRAP.CFG file.

#### Example 4-4

#### Sample NWTRAP.CFG File

```
#
#####
# NWTRAP.CFG
#
# NWTRAP Configuration File
#
# This file specifies information to be used by NWTRAP.NLM
# The file is read and the parameters set when NWTRAP is loaded. It must
# reside on volume SYS: in the directory SYS:\ETC and must be named
# NWTRAP.CFG to be found by NWTRAP. To change the parameters, first edit
# this file, then unload NWTRAP and load it again. Any changes to this file
# will not take effect until NWTRAP is next loaded. The parameters
# are specified by using a parameter keyword followed by the desired
# parameter value.
#
#####

Community
    Public
Time Interval
    10
Severity
    Warning

mask
#     "Memory: Short term alloc failed"
#     1

#     "FileSys: Directory write err (no vol)"
#     2

#     "FileSys: File write err, by server (no path)"
#     3

#     "FileSys: File write err, by user (no path)"
#     4
```

## Defining the Community String

Use the *community* keyword to define the community string to be used in the traps generated. The length of the community string is restricted to 32 bytes and cannot contain space (except between quotes), tab, square bracket, equal sign, colon, semicolon, or number sign (#) characters.

The default string is *public*.

## Setting the Time Interval

Sometimes an alarm repeats rapidly (several times per second or per minute) with identical or nearly identical parameters. When this occurs, the second and later alarms *within a time interval* are *usually* not as interesting as the first alarm.

To prevent the network and the management station from being inundated with identical alarms, you can specify a time interval to be applied to every alarm generated by ManageWise. During this interval, alarms that are identical to an initial alarm are discarded.

You can define the time interval in the configuration file as follows:

**Time Interval**

*n*

where *n* can take any value between 0 and 232, inclusive, to indicate the number of seconds that must elapse before a later alarm is not discarded.

The default time interval is 10 seconds.

## Using Masks

Use the *mask* keyword to provide a list of traps to be disabled. NWTRAP.NLM never forwards these traps to the management stations. You can use a comma (,), a space, or a return (Enter) as a delimiter between trap numbers.

The NWTRAP.CFG file lists each of the traps that can be sent from NetWare Management Agent 2.6 and its trap number. The trap name is

on one line and the trap number is on the following line. The following example shows the first three entries of the mask section in the NWTRAP.CFG file:

```
mask
#   "Memory: Short term alloc failed"
#   1
#   "FileSys: Directory write err (no vol)"
#   2
#   "FileSys: File write err, by server (no path)"
#   3
```

The default state of the file is for these statements to be disabled by placing a number sign (#) before the statement. In addition, the *mask* keyword is not disabled initially because trap 46, *Router configuration error # 1*, is masked out by default.

- ◆ To disable a particular trap, locate it in the NWTRAP.CFG file and remove the number sign preceding the trap number.
- ◆ If you do not want to mask any traps, be sure that the *mask* keyword is disabled to avoid generating an NWTRAP.CFG parse error.

The default is to not disable any specific trap. All traps are sent, except those filtered by the severity level configured.

## Configuring Alarm Severity Levels

Use the *severity* keyword to set a minimum alarm severity level so that traps for lesser severity alarms are not sent.

The severity levels you can set in the NWTRAP.CFG file are *informational*, *warning*, *recoverable*, *critical*, and *fatal*.

When you set a severity level of *informational*, all traps are forwarded. When you set a severity level of *fatal*, no traps are forwarded because there are no fatal traps in the NWTRAP.CFG file.

NetWare defines seven severity levels (adding *operation aborted* and *unrecoverable*). NWTRAP.NLM translates them to the SNMP severity levels shown in Table 4-3. The table also shows the corresponding ManageWise Console severity levels.

**Table 4-3**  
**Comparison of NetWare, SNMP, and ManageWise Severity Levels**

NetWare Severity Level	SNMP Severity Level	ManageWise Console Severity Level
0 - Informational	Informational	Informational
1 - Warning	Minor	Minor
2 - Recoverable	Major	Major
3 - Critical	Critical	Critical
4 - Fatal	Fatal	Critical
5 - Operation Aborted	Fatal	Critical
6 - Unrecoverable	Fatal	Critical

The default is *warning*. Under the default, all alarms with a severity level of *warning* or greater are forwarded.

## Defining Recipients for SNMP Alarms

You can configure NetWare Management Agent 2.6 to send SNMP traps (alarms) to your ManageWise Console or to other management nodes. The NetWare Management Agent software has two ways to determine where to send alarms, which are described in the following sections.

### Automatic Discovery Using FINDNMS.NLM

ManageWise Consoles use the SAP value to identify themselves to NetWare Management Agent 2.6 software installed on NetWare servers. NetWare Management Agent 2.6 uses FINDNMS.NLM on the NetWare server to identify SAP packets being sent by a ManageWise Console and directs traps to that console.

The list of trap-recipient consoles is dynamic. Consoles that do not send SAP packets regularly are removed from the list. The list of trap

recipients is available in the FINDNMS.ADR file in the server's SYS:\ETC directory.

Third-party management consoles that use SNMP over IPX can also use this feature. To do this, they must broadcast the SAP ID number 0x026a periodically. NetWare Management Agent 2.6 then adds their IPX addresses to the list of recipient stations.

## Editing the TRAPTARG.CFG File Manually

In addition to the automatic discovery feature, trap recipients can be added manually to a NetWare server using NetWare Management Agent 2.6. This is useful for having traps sent to network management consoles other than ManageWise, for working with networks where SAP filtering makes automatic discovery impossible, and for receiving traps on networks other than IPX networks.

You must add trap recipients manually by specifying their addresses in the TRAPTARG.CFG file, which is located in the SYS:\ETC directory of all NetWare servers.

The TRAPTARG.CFG file defines the recipients of SNMP traps. You can use this file to define recipients of SNMP traps over IPX and over UDP/IP. The file is fully disabled to show you how to divide the file into IPX and UDP/IP sections and how to write the IPX and IP addresses of recipients.

The TRAPTARG.CFG file is read only when SNMP is loaded. In most cases, this means bringing the server down and restarting it because a variety of modules must be unloaded and reloaded as well. Thus, any changes made to the TRAPTARG.CFG file do not take effect until the next time you load NWTRAP.NLM.

If you are sending traps to third-party management stations, you might need to integrate the NetWare Server trap MIB into those management stations. The MIB can be found in the NWALARM.MIB file on the NetWare Management Agent *Agent Diskette*.

Note



The NWALARM.MIB file imports symbols from the Host Resources MIB (RFC1514.MIB), which is also on the NetWare Management Agent *Agent Diskette*.

Consult your management station documentation for further information about integrating the trap MIB.

## Configuring the ManageWise Console to Not Send SAP Packets

Each ManageWise Console sends a SAP packet with the ID number 0x026a. FINDNMS.NLM uses this packet to identify consoles that it should send traps to. This procedure can create excessive traffic on remote links. This is a particular problem for on-demand, dial-up connections, which can be kept up almost constantly by this process.

To configure the ManageWise Console to not send SAP packets, follow these steps:

Procedure

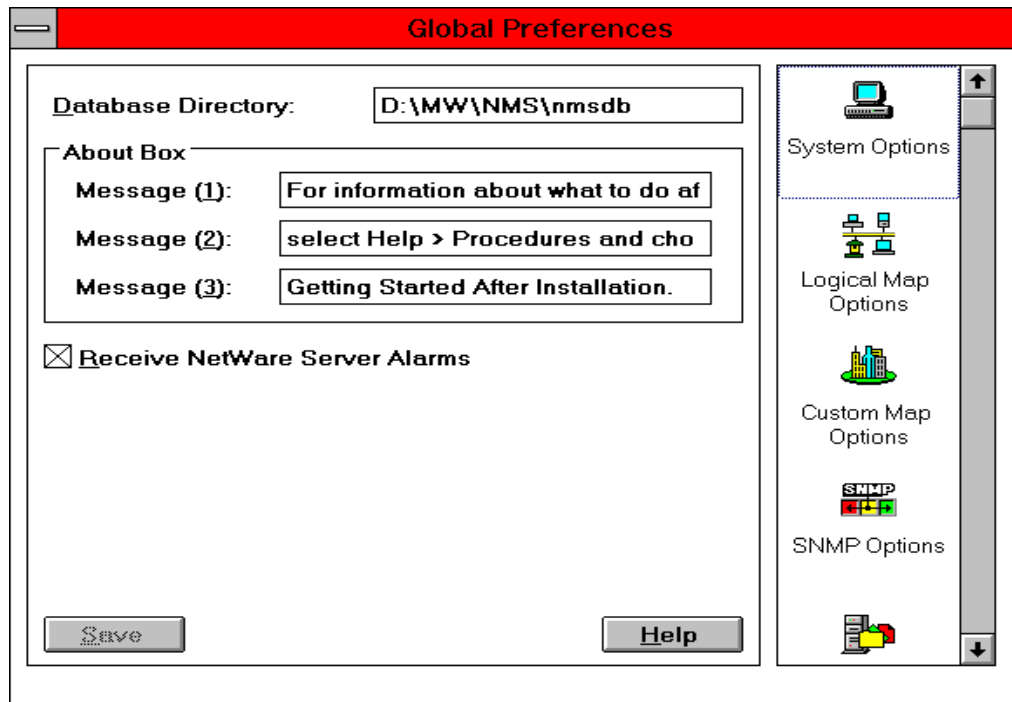


1. **To define the recipients of SNMP traps, follow the instructions in “Editing the TRAPTARG.CFG File Manually” on page 48.**
2. **From the ManageWise Console window, select *Configure > Global Preferences*.**

The System Options Global Preferences dialog page is displayed.

It is identified by the highlighted icon on the right side of the dialog box.

Figure 4-2  
Global Preferences



**3. Deselect the Receive NetWare Server Alarms check box.**

The ManageWise Console no longer sends SAP packets. However, ManageWise might have already sent a SAP packet. In this case, the address of the console is in the server's memory and remains so until it is removed. The default value for removing the console's address is 10 minutes. This value can be altered as described in "Load Parameters for FINDNMS.NLM" on page 35.





# **I**ndex

## **A**

ACTIVATE SERVERS command 12

Aging-out

    default value for 50

Alarm generation 43 to 47

Alarms

    configuring 43 to 47

        recipients 47

        severity levels 46

    masks for 45

    severity levels 47

    time interval 45

## **C**

Community names

    configuration options 26

    defined 24

    false 22

    not encrypted 21

    options 24

    setting up 21 to 28

    unique 21

    using INETCFG 25

Community string

    used by traps 45

Configuring

    alarm generation 43 to 47

    alarm severity levels 46

    alarm time interval 45

    NLM LOAD parameters 31

    sample intervals 38

    security options 23

    security options for ManageWise Console 28

    SNMP alarm recipients 47

    SNMP community names 21 to 28

    SNMP write operations 27

    trend buckets for sample intervals 39

    trends and thresholds 36

## **F**

FINDNMS.NLM file 5, 47, 49

    LOAD parameters for 35

## **G**

GET request 4, 19

## **H**

hardware requirements 8

HOSTMIB.NLM file 4

    LOAD parameters for 32

## **I**

INETCFG, changes to 28

installation 9

    SFT III servers installation procedure 11

    Windows installation procedure 12

Intervals, sample 38

IOAUTO.NCF file 11

IOEngine 11

## L

LOAD command

- configuring parameters for 31
- SNMP options 24

## M

Management by SNMP 2

ManageWise Console

- configuring security 28
- GET operations 28
- limiting SAP packets 49
- SAP number 5, 47
- SET operations 28

Masks for alarms 45

MIBs

- NDSTRAP.MIB file 5
- NWALARM.MIB file 5, 48
- NWHOSTX.MIB file 4
- NWSERVER.MIB file 4
- NWTREND.MIB file 4
- used with NetWare Management Agent 2

MSEngine 11

MSERVERS command 12

## N

NCP. *See* NetWare Core Protocol

NDSTRAP.MIB file 5

NDSTRAP.NLM file 5

NetWare Core Protocol

- SNMP and 20

Netware Core Protocol

- SNMP

- over NetWare Core Protocol 20

NetWare Loadable Module files

- FINDNMS.NLM 5, 35, 47, 49
- HOSTMIB.NLM 4, 32

NDSTRAP.NLM 5

NTREND.NLM 2, 4, 33, 36, 37, 38

NWTRAP.NLM 5, 43

SERVINST.NLM 4, 31

NetWare Management Agent

- hardware requirements 8

installing

- from Windows 12

- SFT III servers 11

NetWare server requirements 8

RAM requirements 8

unloading 15

UNNMA2 command 15

NMA directory 16

NMA2.NCF file 11, 31

NTREND 16

NTREND.INI file 4, 36

- changing threshold values in 41

- returning to initial values 37

NTREND.NLM file 2, 4, 36, 37, 38

- LOAD parameters for 33

NWALARM.MIB file 5, 48

NWHOST.MIB file 4

NWTRAP.CFG file 43, 45

- example of 44

- keywords 44

NWTRAP.NLM file 5, 43

NWTREND.INI, trend values in 37

NWTREND.MIB file 4

## O

On-demand dial-up, limiting traffic 49

## R

RAM

- requirements 8

RCONSOLE 31

requirements

- hardware 8

- NetWare server 8

- RAM 8

## S

- Sample intervals
  - code for 38
  - configuring 38
- SAP number for ManageWise Consoles 5, 47
- Security
  - configuring ManageWise Console for 28
  - configuring options 23
  - SNMP 4, 19
- SERVINST.NLM file 4
  - LOAD parameters for 31
- SET request 4, 19
- SFT III servers
  - ACTIVATE SERVERS command 12
  - installing on 11
  - IOAUTO.NCF file 11
  - IOEngine 11
  - MSEngine 11
  - MSERVERS command 12
  - NMA2.NCF file 11
  - restarting 12
  - synchronizing servers 12
- Simple Network Management Protocol. *See* SNMP
- SNMP
  - alarm recipients 47
  - community names 21
    - configuration options 26
    - configuring 21 to ??, 25, ?? to 28
    - defined 24
    - false 22
  - GET request 4, 19
  - LOAD command options 24
  - management 2
  - security 4, 19
  - SET request 4, 19
  - third-party products and 2
  - trap recipients in TRAPTARG.CFG file 48
  - write operations 27

## T

- Threshold trap, enabling or disabling 43
- Threshold values
  - changing 41
  - configuring 36
  - rising and falling 42
- Traps
  - community string used by 45
  - delimiters 45
  - disabling 45, 46
  - recipients
    - adding 48
    - IPX 48
    - list of 47
    - UDP/IP 48
  - threshold 43
- TRAPTARG.CFG file
  - editing 48
- Trend buckets, specifying 39
- Trend data
  - NTREND.NLM 2
  - stored 2
- Trend file
  - enabling or disabling 41
- Trend values
  - CD-ROM volumes and 37
  - defined 37
  - initial 37
- Trends, configuring 36

## U

- UDP/IP 48
- UNNMA2 command 15

## X

- XCONSOLE 31

